UCSM LDAP故障排除指南

目录

简介

本文档提供有关在统一计算系统管理器(UCSM)上验证轻量级目录访问协议(LDAP)配置的信息，以及调查LDAP身份验证故障问题的步骤。

配置指南：

UCSM配置身份验证

Active Directory(AD)配置示例

验证UCSM LDAP配置

通过检查有限状态机(FSM)状态，确保UCSM已成功部署配置，并显示完成率为100%。

从UCSM命令行界面(CLI)上下文

```
ucs # scope security
ucs /security # scope ldap
ucs /security/ldap # show configuration
ucs /security/ldap # show fsm status
```

从Nexus操作系统(NX-OS)CLI环境

```
ucs # scope security
ucs(nxos)# show ldap-server
```

```
ucs(nxos)# show ldap-server groups
```

LDAP配置最佳实践

1.创建其他身份验证域，而不是更改“本地身份验证”领域

2.始终使用本地领域进行“控制台身份验证”。如果用户使用“本地身份验证”被锁定，管理员仍可从控制台访问。

3.如果给定auth-domain中的所有服务器在登录尝试期间都未能响应，则UCSM始终无法返回本地身份验证（不适用于test aaa命令）。

验证LDAP配置

使用NX-OS命令测试LDAP身份验证。“test aaa”命令仅从NX-OS CLI界面可用。

1.验证LDAP组特定配置。

以下命令根据所有已配置的LDAP服务器的配置顺序浏览其列表。

```
ucs(nxos)# test aaa group ldap <username> <password>
```

2.验证特定LDAP服务器配置

```
ucs(nxos)# test aaa server ldap <LDAP-server-IP-address or FQDN> <username> <password>
```

注释 1：<password>字符串将显示在终端上。

注释 2：LDAP服务器IP或FQDN必须与已配置的LDAP提供程序匹配。

在这种情况下，UCSM会针对特定服务器测试身份验证，如果没有为指定LDAP服务器配置过滤器，则可能会失败。

排除LDAP登录故障

本节提供有关诊断LDAP身份验证问题的信息。

问题场景#1 — 无法登录

无法通过UCSM图形用户界面(GUI)和CLI以LDAP用户身份登录

用户在测试LDAP身份验证时收到“向服务器进行身份验证时出错”。

```
(nxos)# test aaa server ldap <LDAP-server> <user-name> <password>
error authenticating to server
bind failed for <base DN>: Can't contact LDAP server
```

建议
通过互联网控制消息协议(ICMP)ping检验LDAP服务器和交换矩阵互联(FI)管理接口之间的网络连接，并从本地管理情景建立telnet连接

```
ucs# connect local
ucs-local-mgmt # ping <LDAP server-IP-address OR FQDN>
ucs-local-mgmt # telnet <LDAP-Server-IP-Address OR FQDN> <port-number>
```

如果UCSM无法ping通LDAP服务器或打开到LDAP服务器的telnet会话，请检查Internet协议(IP)网络连接。

验证域名服务(DNS)是否为LDAP服务器主机名将正确的IP地址返回给UCS，并确保这两台设备之间未阻止LDAP流量。

问题场景#2 — 可以登录GUI，无法登录SSH

LDAP用户可以通过UCSM GUI登录，但无法打开到FI的SSH会话。

建议

当以LDAP用户身份建立到FI的SSH会话时，UCSM要求在LDAP域名之前预置“ ucs — ”

*从Linux/MAC计算机

```
ssh ucs-<domain-name>\\<username>@<UCSM-IP-Address>
ssh -l ucs-<domain-name>\\<username> <UCSM-IP-address>
ssh <UCSM-IP-address> -l ucs-<domain-name>\\<username>
```

*从putty客户端

```
Login as: ucs-<domain-name>\<username>
```

NOTE:域名区分大小写，并且应与UCSM中配置的域名匹配。最大用户名长度可以是包含域名的32个字符。

"ucs-<domain-name>\<user-name>" = 32个字符。

问题场景#3 — 用户具有只读权限

LDAP用户可以登录，但具有只读权限，即使UCSM中正确配置了ldap组映射。

建议
如果在LDAP登录过程中未检索到任何角色，则根据远程登录策略允许远程用户使用默认角色（只读访问）或拒绝访问（无登录）登录UCSM。

当远程用户登录并授予用户只读访问权限时，在这种情况下，请验证LDAP/AD中的用户组成员身份详细信息。
例如，我们可以对MS Active Directory使用ADSIEDIT实用程序。或ldapserach。

也可以使用NX-OS外壳的“ test aaa”命令来验证。

问题场景#4 — 无法使用“远程身份验证”登录

当“本地身份验证”更改为远程身份验证机制（LDAP等）时，用户无法登录或具有对UCSM的只读访问权限

建议
当UCSM无法到达远程身份验证服务器时，会回退到控制台访问的本地身份验证，因此，我们可以按照以下步骤恢复它。

1.断开主FI的mgmt接口电缆（show cluster state将指示充当主FI的管理接口电缆）
2.连接到主FI的控制台
3.执行以下命令以更改本机身份验证

```
scope security
show authentication
set authentication console local
set authentication default local
commit-buffer
```

4.连接mgmt接口电缆
5.使用本地帐户通过UCSM登录并创建用于远程身份验证（例如LDAP）组的身份验证域。
NOTE:断开管理接口不会影响任何数据平面流量。

问题场景#4 - LDAP身份验证工作，但不启用SSL

没有安全套接字层(SSL),LDAP身份验证工作正常，但启用SSL选项时失败。

建议
UCSM LDAP客户端在建立SSL连接时使用已配置的信任点(证书颁发机构(CA)证书)。

1.确保正确配置了信任点。

2.证书中的标识字段应为LDAP服务器的“主机名”。确保在UCSM中配置的主机名与证书中存在的主机名匹配且有效。

3.确保UCSM配置了LDAP服务器的“hostname”而不是“ipaddress”，并且可以从本地管理接口重新检查。

问题场景#5 - LDAP提供程序更改后身份验证失败

删除旧LDAP服务器并添加新LDAP服务器后，身份验证失败

建议
当LDAP用于身份验证领域时，不允许删除和添加新服务器。从UCSM 2.1版本中，它将导致FSM故障。

在同一事务中删除/添加新服务器时要遵循的步骤是

1.确保使用ldap的所有身份验证领域都更改为本地并保存配置。
2.更新LDAP服务器并验证FSM状态是否已成功完成。
3.将步骤1中修改的域的身份验证领域更改为LDAP。

对于所有其他问题场景 — 调试LDAP

打开调试，尝试以LDAP用户身份登录，并收集以下日志以及捕获失败登录事件的UCSM技术支持。

1)打开到FI的SSH会话，以本地用户身份登录并更改为NX-OS CLI上下文。

```
ucs # connect nxos
```

2)启用以下调试标志并将SSH会话输出保存到日志文件。

```
ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems.
ucs(nxos)# debug aaa aaa-requests

ucs(nxos)# debug ldap all <<< not required, incase of debugging authentication problems.
ucs(nxos)# debug ldap aaa-request-lowlevel
ucs(nxos)# debug ldap aaa-request
```

3)现在打开新的GUI或CLI会话并尝试以远程(LDAP)用户身份登录
4)收到登录失败消息后，**关闭调试。**

```
ucs(nxos)# undebug all
```

LDAP流量的数据包捕获

在需要捕获数据包的情况下，Ethanalyzer可用于捕获FI和LDAP服务器之间的LDAP流量。

```
ucs(nxos)# ethanalyzer local interface mgmt capture-filter "host
```

在上述命令中，pcap文件保存在/workspace/diagnostics目录下，可通过本地管理CLI上下文从FI中检索

以上命令可用于捕获任何远程(LDAP、TACACS、RADIUS)身份验证流量的数据包。
5. UCSM技术支持捆绑包中的相关日志

在UCSM技术支持中，相关日志位**于<FI>/var/sysmgr/sam_logs目录下**

```
httpd.log
```

```
svc_sam_dcosAG
svc_sam_pamProxy.log

NX-OS commands or from <FI>/sw_techsupport log file

ucs-(nxos)# show system internal ldap event-history errors
ucs-(nxos)# show system internal ldap event-history msgs
ucs-(nxos)# show log
```

已知问题说明

CSCth96721
sam上ldap服务器的rootdn应允许128个字符以上

低于2.1的UCSM版本对基本DN /绑定DN字符串有127个字符的限制。

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Guide_2_0_chapter_0111.html#task_0FC4E8245C6D4A64B5A1F575DAEC6127

— 剪刀 —
LDAP层次结构中的特定可分辨名称，当远程用户登录且系统尝试根据用户名获取用户的DN时，服务器应开始搜索。支持的最大字符串长度为127个字符。
—

问题在2.1.1及更高版本中已解决

CSCuf19514
LDAP守护程序崩溃

如果ldap_start_tls_s调用需要60秒以上才能完成初始化，则LDAP客户端在初始化ssl库时可能崩溃。这只有在DNS解析中出现无效DNS条目/延迟时才会发生。

采取措施解决DNS解析延迟和错误。